CAT 2- COMPUTER SYSTEM SECURITY

JOHNSON KANYI- BCSC01/0019/2021

a) Explain THREE checks that a web server may implement to reduce security risks. (6 Marks)

1. **SSL/TLS Encryption**- Encryption of data sent between the server and the clients make information and communication unreadable if intercepted preventing eavesdropping and man in the middle attacks

2. **Regular Security Updates and Patches**- Software updates related to the server and installed applications will keep them updated with the latest patches for known security vulnerabilities.

3. **Firewalls-**
   Firewalls block unauthorized access by monitoring and filtering incoming and outgoing network traffic based on predetermined security rules preventing unauthorized access.

b) Sending a password over a network connection is vulnerable to replay attacks by eavesdroppers. Briefly describe THREE forms of unilateral (or one pass) authentication suitable for human keyboard entry that can reduce that risk with the help of a hardware token and name an advantage for each. (6 Marks)

1. **One-Time Passwords (OTPs):** For every login attempt, the password used is uniquely generated by a hardware token.

   Advantage: It minimizes the possibility of password interception and replay attacks.

2. **Public Key Authentication:** The private key used by the hardware token is mirrored at the server-side with a public key.

   Advantage: The level of authentication will be very strong as there will be no transmission of the private key.

3. **Biometric Authentication:** The hardware token contains a biometric scanner such as for fingerprint.
   Advantage: Guarantees another level of security that is the need for physical presence.

c) An application process receives information via a UDP packet over a wired Ethernet LAN connection. If the packet carries a source port number below 1024, under which conditions can the information be trusted. (4 Marks)

1. The ***network is isolated*** or secured-such as on a trusted wired Ethernet LAN. The network under which the UDP packet is transmitted is isolated from the internet (***its is a private network***)
2. The ***source system*** enforces restrictions using its security configurations, as ports below 1024 are typically reserved for privileged processes (e.g., root/administrator-level in UNIX systems or HTTP on port 80 or HTTPS on port 443 as trusted services).
3. The packet is validated through other mechanisms, such as ***cryptographic authentication, security certificates or firewalls.***

d) Describe a UDP-based amplification attack, and why are similar attacks far less practical via TCP. (4 Marks)

The attack would be carried out by having an attacker send a **small query** as request to a server with a **spoofed IP address** of the victim. The server then sends a much larger response to the victim, overwhelming his or her system. This is possible because UDP is a ***connectionless*** protocol hence it requires no handshake or set-up connection, making IP address spoofing very easy.

TCP being a **connection-oriented protocol** unlike UDP, requires a connection (the handshake process) to be established before data is sent, this makes spoofing IP addresses harder; therefore, similar types of attacks are less practical via TCP.

e) Compare and contrast between LINUX operating systems and WINDOWS operating systems security features. (4 Marks)

1. ***User Permissions:***

LINUX has ***fine-grained file permissions***, with separate permissions for read, write, and execute for the owner, group, and others **whereas** in **WINDOWS**, it depends on ***User Access Control*** to manage privileges of programs and users making it centralized but less customizable.

2. ***Open-source code:***

   The **open-source kernel** within **LINUX** lets the world community of ***developers' patch vulnerabilities*** at incredible speed and ensures timely security updates while in **WINDOWS** relies upon ***vendor-provided updates***, sometimes well after the fact.

3. ***Default Security:***

   LINUX systems, by default, ***install only the necessary running services***, which minimizes the attack surface whereas **WINDOWS** installs a ***lot of software and services***, increasing the attack surface but centrally managed for usability and integration.

f) Explain THREE ways in which you can prevent hacking of your social media accounts. (6 Marks)

1. By using **strong, unique Passwords**: Create complex passwords with a mix of letters, numbers, and special characters.
2. **Two-Factor Authentication (2FA)** Enabled: add a second layer of verification as an extra line of defence.
3. **Keep Social Media Applications as well as the software updated** that is operating systems and web browsers of the device being used to access the applications. This will prevent exploitation of known security flaws in outdated software.